



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,472	01/26/2001	Jean Louis Calvignac	RAL920000119US1	6208
25299	7590	06/30/2008		
IBM CORPORATION PO BOX 12195 DEPT YXSA, BLDG 002 RESEARCH TRIANGLE PARK, NC 27709			EXAMINER TRAN, ELLEN C	
			ART UNIT	PAPER NUMBER
			2134	
			MAIL DATE	DELIVERY MODE
			06/30/2008 PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary**Application No.**

09/771,472

Applicant(s)

CALVIGNAC ET AL.

Examiner

ELLEN TRAN

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 04 April 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
- 4) ☐ Interview Summary (PTO-413)
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____
- 7) ☐ Paper No(s)/Mail Date: _____

DETAILED ACTION

1. This action is responsive to: communication filed on 4 April 2008, with acknowledgement of an original application filed 26 January 2001.
2. Claims 1-25 are currently pending in this application. Claims 1, 16, 19, and 21 are independent claims. Claims 22-25 are new. Amendments to the claims and drawings are accepted.

Response to Arguments

3. Applicant's arguments with respect to 1-26 have been considered but they are not persuasive. The Objection to the drawings has been removed due to amendment.
- I) In response to Applicant's argument beginning on page 10, "*Claims 1, 10-16 and 18-21 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 7,254,231 to VAN DYKE et al. Applicant respectfully traverses this rejection ... In particular, independent claims 1, 16, 19, and 21 recite: ... the combinational logic comprising logic function whose outputs depend solely on their inputs and utilizing logic circuits without memory ... However, the Examiner is not correct that the general processor (which utilizes ALUs 302, 304, and 306) of VAN DYKE, discussed on col. 4, lines 5-29 and col. 5, line 58 to col. 6, line 2, can be properly characterized as the recited combinational logic comprising logic functions whose outputs depend solely on their inputs and utilizing logic circuits without memory. It is clear from the very language cited by the Examiner that the general processor includes pipe line stage 37 which is described as a memory stage ... As general processor 302/304/306 utilizes memory stage 37, the Examiner is not correct that such a device can be properly characterized as the*

recited combinational logic comprising logic functions whose outputs depend solely on their inputs and utilizing logic circuits without memory”.

The Examiner disagrees with argument below is the text from the Van Dyke reference col. 5, line 58 through col. 6, line 2: “In this embodiment, bypass mechanisms are provided in ALU 302, so that the results of logic circuit 309 and shifter 314 can each be provided back as input values to ALU 302. If the programmer uses the same corresponding general purpose registers for sources and destinations, all sixteen rounds of DSTEP can be executed using the bypass mechanism--i.e., no register write back time (i.e., latency of instruction execution pipeline stage 38) is required, thereby providing even higher performance. Bypass mechanisms are also provided elsewhere in ALUs 302, 304, and 306, so results may be immediately used as operands without delaying through instruction execution pipeline stage 38”. The result of the logic circuit and shifter (i.e. combination logic) are provided back as input values, no register write back time. This “bypass mechanism” has the same meaning as “whose outputs depend solely on their inputs and utilizing logic circuits without memory”.

II) In response to Applicant’s argument beginning on page 13, “Claims 2-9 and 17 are rejected under 35 U.S.C. . § 103(a) for *being allegedly unpatentable over VAN DYKE in view of US Patent No. 6,704,871 to KAPLAN et al. This rejection is respectfully traversed ... Applicant submits that this rejection is improper at least because KAPLAN fails to cure the deficiencies of VAN DYKE”.*

The Examiner disagrees with the argument because Van Dyke teaches the bypass mechanism which uses combinational logic circuits without memory.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(c) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

5. **Claims 1, 10-16, and 18-25** are rejected under 35 U.S.C. 102(c) as being anticipated by Van Dyke et al. U.S. Patent No. 7,254,231 (hereinafter ‘231).

As to independent claim 1, “A hardware implementation of a crypto-function comprising: a first register storing data to be encrypted or decrypted” is taught in ‘231 col. 6, lines 12-29;

“a second register for receiving data which has been encrypted or decrypted” is shown in ‘231 col. 6, lines 37-44;

“and combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle” is disclosed in ‘231 col. 4, lines 5-29;

“wherein the combinational logic comprises logic functions whose outputs depend solely on their inputs and utilizes logic circuits without memory” is taught in ‘231 col. 5, line 58 through col. 6, line 2.

As to dependent claim 10, “wherein the hardware implementation of the crypto-function uses only the combinational logic without having to store intermediate results in registers” is shown in ‘231 col. 5, line 58 through col. 6, line 2.

As to dependent claim 11, wherein the hardware implementation the crypt-function computes an iterated round function in one clock cycle” is disclosed in ‘231 col. 5, line 58 through col. 6, line 2.

As to dependent claim 12, “wherein the combination logic utilizes a Data Encryption Standard (DES) algorithm that is implemented in the combination logic” is taught in ‘231 col. 3, lines 29-35.

As to dependent claim 13, “wherein the combination logic utilizes logic functions whose outputs depend solely on their inputs” is shown in ‘231 col. 5, line 58 through col. 6, line 2.

As to dependent claim 14, “wherein the combination logic utilizes logic circuits without memory, whereby no registers are used to store intermediate results or iterations of encipher or deciphering computations” is taught in ‘231 col. 5, line 58 through col. 6, line 2.

As to dependent claim 15, “wherein the crypt-function is implemented in the combinational logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read” is shown in ‘231 col. 5, line 58 through col. 6, line 2.

As to independent claim 16, “A hardware implementation of a crypto-function comprising: a first register that stores data to be encrypted or decrypted” is taught in ‘231 col. 6, lines 12-27;

“a second register that receives data which has been encrypted or decrypted” is shown in ‘231 col. 6, lines 37-44;

“and combinational logic that performs computation iteration of the crypto-function on data store in the first register and outputting data to said second register in a single hardware cycle, the combinational logic comprising logic functions whose outputs depend solely on their inputs and utilizing logic circuits without memory, wherein the crypt-function without intermediate registers that require loading and settling time before contents of the intermediate registers can be read” is disclosed in ‘231 col. 4, lines 5-29 and col. 5, line 58 through col. 6, line 2.

As to dependent claim 18, wherein the hardware implementation of the crypto-function computes and iterated round in just one clock cycle” is disclosed in ‘231 col. 5, line 58 through col. 6, line 2.

As to independent claim 19, “A hardware implementation of a crypto-function comprising: a first register that stores data to be encrypted or decrypted” is taught in ‘231 col. 6, lines 12-29;

“a second register that receives data which has been encrypted or decrypted” is shown in ‘231 col. 6, lines 37-44;

“and combination logic that performs computation iteration of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle” is disclosed in ‘231 col. 4, lines 5-29;

“the combination logic comprising logic functions whose outputs depend solely on their inputs and utilizing logic circuits without memory, wherein the single hardware cycle comprises several clock cycles” is taught in ‘231 col. 5, line 58 through col. 6, line 2.

As to dependent claim 20, **“wherein the crypto-function is implemented in the combination logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read”** is shown in ‘231 col. 5, line 58 through col. 6, line 2.

As to independent claim 21, **“A hardware implementation of a crypto-function comprising: a first register storing data to be encrypted or decrypted, wherein the inputs to the first register are bits from an initial value accumulator, a data register, and a key register”** is taught in ‘231 col. 6, lines 12-29;

“combination logic performing computational iterations of the crypto-function on data stored in the first register and outputting data to a second register in a single hardware cycle” is disclosed in ‘231 col. 4, lines 5-29;

“bits from the initial value accumulator and the data register are exclusive ORed and then subjected to an initial permutation in a permutation logic” is taught in ‘231 col. 4, lines 25-67;

“an output of the permutation logic comprising a logic block performing a key-dependent computation which involves the key schedule” is shown in ‘231 col. 5, lines 41-55;

“and an output key register being subject to a permutation choice in another permutation logic” is disclosed in ‘231 col. 4, lines 41-67;

“wherein the combination logic comprises logic functions whose outputs depend solely on their inputs and utilizes logic circuits without memory” is taught in ‘231 col. 5, line 58 through col. 6, line 2.

As to dependent claim 22, “wherein the crypto-function utilizes sixteen rounds and produces a final output” is shown in ‘231 col. 5, lines 58-66.

As to dependent claims 23-25, these claims contain substantially similar subject matter as claim 22; therefore they are rejected along similar rationale.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. **Claims 2-9 and 17**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Van Dyke et al. U.S. Patent No. 7,254,231 (hereinafter ‘231) in view of Kaplan et al. U.S. Patent No. 6,704,871 (hereinafter ‘871) .

As to dependent claim 2, the following is not explicitly taught in ‘231: “wherein the crypto-function is a block cipher algorithm” however ‘871 teaches that the DES algorithm comprises block cipher algorithm in col. 10, lines 15-17.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a hardware implementation of a crypto-function taught in '231 to include a means to utilize a digital signal processor (DSP) that implements various encryption algorithms. One of ordinary skill in the art would have been motivated to perform such a modification because of the growing use of DSP and the security needed with transmission see '871(col. 1, lines 30 et seq.) "Digital signal processors (DS) are widely used in devices such as modems, cellular telephones and facsimiles. With an increase in digital communications, data transmission security has become an issue in numerous DSP applications. A standard DSP is not capable of providing data transmission security; thus additional hardware and software are required".

As to dependent claim 3, "wherein the crypto-function is the Data Encryption Standard (DES) algorithm" is shown in '231 col. 3, lines 29-35 and '871 col. 10, lines 15-17.

As to dependent claim 4, "wherein the crypto-function is the CHAIN algorithm" is disclosed in '871 col. 10, lines 15-17.

As to dependent claim 5, "wherein the combinational logic performs an invertible key-dependent round function iterated a predetermined number of times" is taught in '231 col. 1, line 57 through col. 2, line 29.

As to dependent claim 6, "wherein the combination logic performs mixing, permutation and key-dependent substitution in each round" is shown in '231 col. 1, line 57 through col. 2, line 29.

As to dependent claim 7, "wherein the combinational logic enciphers a block by performing an initial permutation of a block to be enciphered and then a complex key-

dependent computation followed by a permutation which is an inverse of the initial permutation” is disclosed in ‘231 col. 1, line 57 through col. 2, line 29.

As to dependent claim 8, “wherein the combinational logic deciphers a block by performing deciphering using the same key as used to encipher the block in a process that is an inverse of the enciphering process” is taught in ‘231 col. 1, lines 11-29.

As to dependent claim 9, “wherein the one hardware cycle is approximately ten clock cycles” is shown in ‘871 col. 10, lines 13-25.

As to dependent claim 17, “wherein the single hardware cycle is approximately ten clock cycles” is disclosed in ‘871 col. 10, lines 13-25.

Conclusion

Accordingly, THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

8. It is noted, PATENTS ARE RELEVANT AS PRIOR ART FOR ALL THEY CONTAIN “The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain.” In re Heck, 699 F.2d 1331, 1332-33, 216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting In re Lemelson, 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA 1968)). A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including nonpreferred embodiments (see MPEP 2123).
9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 7:30 am to 4:00 pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/ELLEN TRAN/
Primary Examiner, Art Unit 2134
25 June 2008